Board of Governors of the Federal Reserve System

REPORT ON THE AUDIT OF THE BOARD'S IMPLEMENTATION OF ELECTRONIC AUTHENTICATION REQUIREMENTS

OFFICE OF INSPECTOR GENERAL

March 2006

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

OFFICE OF INSPECTOR GENERAL

March 31, 2006

The Honorable Mark W. Olson
Chairman, Committee on Board Affairs
Board of Governors of the Federal Reserve System
Washington, DC 20551

Dear Governor Olson:

The Office of Inspector General (OIG) is pleased to present its *Report on the Audit of the Board's Implementation of Electronic Authentication Requirements.* We began this audit as part of an effort to perform work throughout the year related to our independent evaluation responsibilities under the Federal Information Security Management Act (FISMA) and in response to questions from the Office of Management and Budget (OMB) as part of previous FISMA reporting guidance regarding the agency's progress in completing electronic authentication (e-authentication) risk assessments. Our objectives were to (1) determine whether the Board of Governors of the Federal Reserve System (Board) appropriately identified the systems requiring e-authentication risk assessments, (2) determine whether the Board prepared assessments in accordance with guidance issued by OMB and the National Institute of Standards and Technology, and (3) evaluate how e-authentication requirements are being included in the Board's revised information security program.

We found that the Board identified and completed e-authentication risk assessments for seven applications that provide access to remote users. However, we identified at least two additional applications accessed by other government agencies and third parties outside the Federal Reserve System for which e-authentication risk assessments were not completed. In addition, we found that the risk assessments prepared for the seven applications were not consistently completed across divisions and that five of these assessments had variations from OMB guidance. Because the Board's information security program was in a period of transition at the time the assessments were completed, the Information Security Officer (ISO) had not developed specific e-authentication guidance, and related guidance (such as procedures for risk assessments and certification and accreditation) had not been finalized. The seven e-authentication assessments were completed primarily to fulfill a specific OMB annual reporting requirement, as opposed to being an integral part of a broader information security lifecycle framework.

During our audit fieldwork, we shared our initial observations with the Board's information security staff and the ISO has incorporated our input into a revised risk assessment guide, which includes specific e-authentication guidance. The draft guidance, dated February 2006, addresses many of the issues identified during the audit and provides additional information to assist system owners in completing the e-authentication risk assessments once the requirement for an

assessment has been determined. The e-authentication risk assessments will now be part of the overall risk assessment process which should help ensure that all systems meeting the e-authentication requirements have been identified. The ISO also told us that the Board's revised certification and accreditation process will include procedures to confirm that systems achieve the required e-authentication assurance level and that the e-authentication process satisfies a system's authentication requirements. In addition, annual information security control reviews will reassess systems to ensure that the authentication requirements remain valid as a result of technology changes or changes in the Board's business practices. Our report contains a recommendation for the Chief Information Officer (CIO) to finalize the e-authentication guidance, including processes for validating and periodically reassessing assurance levels, and to ensure that all applications meeting e-authentication requirements are identified and properly assessed.

We provided a copy of our report to the director of the Division of Information Technology, who serves as the Board's CIO for FISMA purposes, for review and comment. In her response, the director concurs with our recommendation and describes several actions underway or already completed to finalize the Board's e-authentication guidance and implement the related procedures. We will follow up on actions taken as part of future audit work related to information security.

We are providing copies of this audit report to Board management officials. The report will be added to our public web site and will be summarized in our next semiannual report to the Congress. Please contact me if you would like to discuss the audit report or any related issues.

Sincerely,

/signed/

Barry R. Snyder
Inspector General

Enclosure

cc: Governor Donald L. Kohn
Governor Randall S. Kroszner
Mr. Stephen Malphrus
Ms. Marianne Emerson

Board of Governors of the Federal Reserve System

REPORT ON THE AUDIT OF THE BOARD'S IMPLEMENTATION OF ELECTRONIC AUTHENTICATION REQUIREMENTS

OFFICE OF INSPECTOR GENERAL

March 2006

TABLE OF CONTENTS

Page

BACKGROUND

On December 17, 2002, the E-Government Act of 2002, Public Law 107-347 (E-Gov Act) was enacted to, among other things, enhance citizen access to government information and services and to improve government operations; primarily through expanded use of the Internet. The E-Gov Act requires each agency to ensure that the methods it uses to secure access to electronic government information and services are in accordance with relevant policies and procedures issued by the Director of the Office of Management and Budget (OMB) and applicable technical guidance developed by the National Institute of Standards and Technology (NIST). These policies, procedures, and guidance encompass electronic authentication (e-authentication), or the process an agency uses to validate the identity of users attempting to gain system access. E-authentication focuses on determining a user's identity; it does not refer to "authorization," which focuses on the user's permissions once access to a system has been granted.

To fulfill its responsibilities, OMB issued, in December 2003, Memorandum M-04-04 entitled *E-Authentication Guidance for Federal Agencies*. M-04-04 requires agencies to review new and existing electronic transactions to ensure that authentication processes provide an appropriate level of assurance regarding a user's identity. To implement this requirement, M-04-04 directs agencies to conduct risk assessments and determine the potential harm or impact that might result from an authentication error; that is, having someone who is not who they claim to be gain access to a system. Based on the risk assessment, agencies must determine the required level of authentication assurance for each transaction and then select the appropriate technology to achieve that assurance level using technical guidance in NIST Special Publication 800-63, *Electronic Authentication Guidance*. OMB's guidance also requires agencies to validate that the system has achieved the required assurance level and then periodically reassess the system to determine any technology refresh requirements. M-04-04 directed all agencies to categorize all existing transactions and systems requiring e-authentication into one of the described assurance levels by September 15, 2005. Appendix I to this report provides additional information regarding M-04-04.

The E-Gov Act also includes the Federal Information Security Management Act (FISMA), which lays out a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. FISMA assigns responsibility to the agency's Chief Information Officer (CIO) to ensure compliance with FISMA's requirements, and requires the Office of Inspector General (OIG) to perform an annual independent evaluation of the agency's information security program and practices. To assist agencies in fulfilling their FISMA evaluation and reporting responsibilities, OMB issues annual reporting guidance. The guidance emphasizes reporting based on security-related measures, and OMB has begun incorporating additional requirements into the agencies' annual FISMA reporting. For the past two reporting periods, OMB has specifically requested information on each agency's progress in implementing e-authentication requirements.

The Board of Governors of the Federal Reserve System (Board) has designated the Staff Director for Management as the Board's CIO. The Staff Director has delegated to the director of the

Division of Information Technology (IT) certain CIO functions pertaining to FISMA and E-Government. An IT assistant director serves as the Board's Information Security Officer (ISO) and is the focal point for the Board's information security activities, including risk assessments, certification and accreditations, and annual control testing. Because much of the information technology at the Board is decentralized, individual divisions and offices also have information security responsibilities.

OBJECTIVES, SCOPE, AND METHODOLOGY

We began this audit as part of an effort to perform work throughout the year related to our independent evaluation responsibilities under FISMA. We conducted audit fieldwork from December 2005 through February 2006. Our objectives were to (1) determine whether the Board appropriately identified the systems requiring e-authentication assessments, (2) determine whether the Board prepared assessments in accordance with guidance issued by OMB and NIST, and (3) evaluate how e-authentication requirements are being included in the Board's revised information security program. To accomplish our objectives, we compared Board policies and procedures with OMB and NIST guidance, interviewed IT security staff and system owners, and reviewed completed e-authentication risk assessments. Our audit was conducted in accordance with generally accepted government auditing standards.

FINDINGS AND OBSERVATIONS

As of December 31, 2005, the Board had identified eight applications that provide access to remote users and were, therefore, subject to e-authentication requirements. Seven applications are maintained by the Board, and support functions ranging from banking supervision to currency distribution. These applications are accessed by other government agencies, commercial vendors, and financial institutions. For these seven applications, system owners completed e-authentication assessments using a template provided by the Board's ISO. The eighth application, maintained by the Federal Reserve Bank of New York, did not undergo an e-authentication risk assessment although it was identified as being subject to e-authentication requirements.

Board staff completed the e-authentication risk assessments during a period of transition for the Board's information security program. At that time, the ISO had not developed specific guidance for performing e-authentication assessments, and related guidance (such as procedures for system risk assessments and certification and accreditation) had not been finalized. The e-authentication assessments were completed primarily to fulfill a specific OMB annual reporting requirement, rather than as part of a broader information security lifecycle framework. OMB's 2005 FISMA reporting guidance states the e-authentication risk assessments should be conducted in parallel with the overall system risk assessment and in the context of greater policy issues; the assessments should be conducted with the advice of agency legal, policy, privacy, and agency business owners. In our opinion, completing the e-authentication template outside the overall risk assessment processes did not provide adequate assurance that all applications

requiring e-authentication risk assessments were identified or that the risk assessments were completed consistently across divisions and in accordance with OMB requirements.

Our review of the Board's application inventory and application security plans identified at least two additional applications accessed by other government agencies and other third parties outside the Federal Reserve System (System) for which e-authentication risk assessments were not completed. We also found that divisions inconsistently applied the concept of "remote access" to applications accessed by Reserve Bank personnel. (At the time these assessments were completed, the Board had not yet clearly defined the applicability of e-authentication to remote access by Reserve Bank staff.) As a result, one division included some, but not all, applications where the only third-party access is by Reserve Bank staff; other divisions did not include any applications with similar access.

We also found that the seven assessments were not consistently completed across divisions and that five of these assessments had variations from OMB guidance. For example, we found that divisions were inconsistent in identifying the types of transactions or functions that application users were able to perform once they were granted access; identifying the transaction or function is one of the first steps in completing the risk assessment process. We also found that one division did not properly assess potential impact categories and that one of the tables in the template provided to the system owners was inconsistent with M-04-04. [1] Our discussions with individuals completing the assessments also showed the lack of a clearly defined process for assigning assurance levels. In addition, the assessments did not identify the corresponding technical requirements needed to achieve the level of assurance indicated by the assessment.

During our audit fieldwork, we shared our initial observations with the Board's information security staff; the ISO incorporated our input in drafting a new risk assessment guide which includes specific e-authentication guidance. The draft e-authentication guidance prepared as of February 2006 addresses many of the issues discussed above. For example, consistent with OMB requirements, the draft guidance requires that information system owners complete an e-authentication assessment for all Board information systems that provide access to remote users via the Internet—including information systems developed and operated on behalf of the Board by third parties. The draft guidance defines remote users as the public, state government, commercial financial institutions, and other Federal government agencies. The guidance also defines remote access as occurring when a user is permitted to directly access a Board information system from outside the System network, which includes the Board as well as the twelve Reserve Banks. System personnel who access Board information systems through the System's intranet are, thus, not considered remote users, since the Board and the System share a trusted network and, thus, the Board trusts the System's authentication of its staff.

The draft guidance also provides additional information to assist systems owners in completing the e-authentication risk assessment once the requirement for an assessment has been determined. The ISO has revised the table that was inconsistent with OMB guidance and has provided additional guidance for properly identifying transactions and functions. The

[1] Required assurance levels are determined by assessing the potential impact of categories of harm listed in M-04-04 using impact values described in Federal Information Processing Standard 199, "Standards for Security Categorization of Federal Information and Information Systems."

e-authentication risk assessments will now be part of the overall risk assessment process which should help ensure that all applications meeting the e-authentication requirements have been identified. In our opinion, the changes should help promote both greater consistency across divisions and compliance with OMB requirements.

RECOMMENDATION

We recommend that the CIO: (1) finalize e-authentication guidance, to include providing additional guidance regarding assurance levels; (2) ensure that all applications meeting e-authentication requirements are identified and properly assessed; and (3) ensure that procedures are in place to include the validation and periodic reassessment of assurance levels as part of the Board's revised information security program.

We understand that the ISO is awaiting input from the Board's Legal Division (Legal) before finalizing the guidance. We encourage information security and Legal staffs to complete the revision process to ensure that the Board's revised information security program (to include e-authentication) is implemented within the Board's milestone objectives in order to maintain compliance with all legislative and regulatory requirements. In finalizing the guidance, we believe the ISO and Legal need to ensure that the treatment of the "System network" for e-authentication purposes is consistent with the Board's treatment of the network for other information security purposes, especially since the Board considers that the Reserve Banks are third parties with respect to FISMA, and that their networks are not directly subject to FISMA requirements.

One other area where we believe additional guidance is required is establishing criteria for assigning assurance levels to potential impact categories for authentication errors. Our review of the completed e-authentication assessments found that for some systems containing restricted-controlled supervisory information, Board staff assigned a low assurance level to the potential impact category of "unauthorized sensitive information."[2] A low assurance level is appropriate when release of the information would cause minor inconvenience or minor risk or harm to Board programs. We believe that a low assurance level is inconsistent with other Board classification guidelines and that any system containing restricted-controlled data should be assigned at least a moderate assurance level. We believe this treatment would be consistent with M-04-04 which requires a similar approach for assessing the potential impact category of "personal safety."

Finally, the draft guidance does not specifically address the implementation of technical solutions to achieve the required level of assurance or the verification process necessary to ensure that the solutions have been properly implemented and are functioning as intended. Because some implementations may create or compound particular risks, a final validation is needed to confirm that the system achieves the required assurance level. The Board must also periodically reassess the information system to ensure that the authentication requirements

[2] Restricted-controlled is a Board information classification for information that should only be shared with System staff that are authorized and have a need to know the information for official business purposes.

remain valid and are functioning properly. The ISO told us that the Board's revised certification and accreditation process will include procedures to confirm that the system achieves the required assurance level and that the e-authentication process satisfies the system's authentication requirements. In addition, the ISO indicated that annual information security control reviews will reassess the system to ensure that the authentication requirements remain valid as a result of technology changes or changes in the Board's business practices. Ensuring that e-authentication is properly incorporated into these other information security processes will be essential to maintaining a robust assessment function.

ANALYSIS OF COMMENTS

We provided our report to the Director of IT, in her capacity as CIO for FISMA, and her response is included as appendix 2. In her response, the director concurs with our recommendation and describes several actions underway or already completed. Specifically, the director notes that the Board's e-authentication guidance will be finalized by March 31, 2006, and will include additional criteria for assigning assurance levels. The director also notes that the Board's certification and review procedures will include steps to ensure that the technical solution employed for a system achieves the required level of assurance. In addition, the director's response describes existing controls over access to Board systems by Reserve Bank staff and the reasons that she believes the Board is consistent with its treatment of the "System network" for e-authentication and other information security purposes, including FISMA. We will follow up on actions taken related to our recommendation as part of future audit work related to information security.

APPENDIXES

Appendix 1 – OMB's E-Authentication Guidance

To implement Section 203 of the E-Government Act and to help agencies provide secure electronic services that protect individual privacy, OMB issued, in December 2003, Memorandum M-04-04 entitled, *E-Authentication Guidance for Federal Agencies*. In September 2004, NIST issued Special Publication 800-63, *Electronic Authentication Guideline* to supplement OMB guidance and provide technical guidance.

Specifically, Memorandum M-04-04 requires agencies to review new and existing electronic transactions to ensure that the authentication processes provide the appropriate level of assurance. It establishes and describes four levels of identity assurance for electronic transactions requiring authentication. These levels represent ranges of confidence in establishing the identity of an individual attempting to access a system. The four levels are:

1 - little or no confidence in the asserted identity's validity,
2 - some confidence in the asserted identity's validity,
3 - high confidence in the asserted identity's validity, and
4 - very high confidence in the asserted identity's validity.

Memorandum M-04-04 instructs agencies how to implement the e-authentication requirements by outlining a process for assessing risk, describing four levels of identity assurance, and explaining how to determine the appropriate level of identity assurance. The guidance outlines a process for determining the level of e-authentication assurance required for specific applications and transactions, based on the risks and their likelihood of occurrence for each application or transaction. Agencies are to determine assurance levels using the following steps:

- conduct a risk assessment of the system,
- map identified risks to the applicable assurance levels,
- select technology based on NIST guidance,
- validate that the system has achieved the required assurance level, and
- periodically reassess the system to determine technology refresh requirements.

<u>Conducting a risk assessment:</u>
To assign the appropriate assurance level for e-authentication, the system owner must assess the potential risks and corresponding harm, and then identify measures to minimize their impact. Categories of harm and impact include:

- inconvenience, distress, or damage to standing or reputation,
- financial loss or agency liability,
- harm to agency programs or public interests,
- unauthorized release of sensitive information,
- personal safety, and
- civil or criminal violations.

Appendix 1 – OMB's E-Authentication Guidance

Mapping risks to the applicable assurance level:
The required assurance levels for electronic transactions are determined by assessing the potential impact of each of the above categories using the potential impact values described in Federal information Processing Standard (FIPS) 199, *Standards for Security of Federal Information and Information Systems*. The three potential impact values are:

- Low impact
- Moderate impact
- High impact

Memorandum M-04-04 defines the potential impacts for each category. For example, the potential impacts for the category of "inconvenience, distress, or damage to standing or reputation" are:

- **Low** – at worst, a limited, short-term inconvenience, distress or embarrassment to any party.

- **Moderate** – at worst, a serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party.

- **High** –a severe or serious long-term inconvenience, distress, or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals).

Agencies must then compare the impact profile from the system's risk assessment to the impact profiles associated with each of the four assurance levels as shown in the following table. Agencies should choose the lowest level that will cover all of the potential impacts.

Assurance Levels (1 through 4)

Potential Categories for Authentication Errors	**1**	**2**	**3**	**4**
	Impact Ratings			
Inconvenience, distress, damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod/High
Civil or criminal violations	N/A	Low	Mod	High

Appendix 1 – OMB's E-Authentication Guidance

Selecting the appropriate technology:
After determining the assurance level, agencies must refer to NIST e-authentication technical guidance in SP 800-63 to identify and implement the appropriate requirements. NIST 800-63 provides the technical requirement for each of the four levels.

- Level 1 - no proofing requirement, but the authentication mechanism used provides some assurance. A user registers and creates a simple password, but the user's identity is not verified.

- Level 2 - provides single factor remote network authentication. A user registers, the user's identity is verified, and the user is provided a password or PIN.

- Level 3 - provides multi-factor remote network authentication. A user registers, the user's identity is verified, and the user is provided a password or PIN, as well as a token, such as a key.

- Level 4 - is the highest practical network authentication assurance. A user registers, the user's identity is verified, and the user is provided a password or PIN, as well as a physical token, such as a biometric.

Appendix 2 – Division Director's Comments

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
OFFICE OF INSPECTOR GENERAL

DATE: March 30, 2006

TO: Mr. Barry R. Snyder

FROM: Marianne M. Emerson */signed/*

SUBJECT: Comments on the Office of the Inspector General's Audit of the Board's Implementation of Electronic Authentication Requirements.

Thank you for the opportunity to comment on the Office of the Inspector General's (OIG's) audit of the Board's Implementation of Electronic Authentication Requirements. We generally concur with the findings and observations of the audit. As the audit report highlights, E-Authentication guidance has been integrated into the Board's new risk assessment process. As such, E-Authentication risk assessments will now be conducted as part of the overall system risk assessment which should help improve completeness and consistency.

The following is our response and comments to the audit report's single recommendation. The recommendation is set forth in bold face below, accompanied by our comments, which refer not only to the recommendation itself, but also to the accompanying justification language in the audit.

Recommendation: We recommend that the CIO: (1) finalize e-authentication guidance, to include providing additional guidance regarding assurance levels; (2) ensure that all applications meeting e-authentication requirements are identified and properly assessed; and (3) ensure that procedures are in place to include the validation and periodic reassessment of assurance levels as part of the Board's revised information security program.

Response: We concur with the recommendation. The Board's E-Authentication guidance will be finalized by March 31, 2006. The guidance will also include additional criteria for assigning assurance levels as recommended by the audit team.

In finalizing the guidance, we consulted with Legal regarding our treatment of the "System network" for e-authentication purposes and believe that we are being consistent with our treatment of the network for other information security purposes, including FISMA. Specifically, the E-Authentication Guidelines issued by the National Institute of Standards and Technology (NIST), Special Publication 800-63, are aimed at remote authentication of users over open networks. This is also our assessment of the intent of OMB guidance contained in

Appendix 2 – Division Director's Comments

Memorandum 04-04. OMB's guidance is aimed specifically at E-Government systems that provide services via the Internet. Access by Reserve Banks to the Board does not pose these same issues as the access is allowed through a closed network. While not subject to FISMA, the Banks have implemented controls regarding access to their internal network which is considered to be a closed network. These include physical access controls, logical access controls, technical controls, and management controls. Consequently, when Reserve Bank staff access a Board system, the access is performed via a physically secure device provided by a System-managed network that shares an interconnection to the Board's closed network. The controls in place for this access, including those provided by Active Directory, meet Level 3 authentication requirements and thus are sufficient to allow access to Board systems requiring up to a Level 3 authentication. Board systems with higher authentication and access controls are secured through additional requirements that are imposed on all internal users. Moreover, when Bank staff access the Bank network remotely via the Internet, they must use the National Remote Access System (NRAS), based on a two-factor authentication, that meets Level 4 authentication requirements. Thus, we determined that performing separate E-Authentication assessments for each Board system accessed by Reserve Bank staff via InterFed is not necessary as the existing controls meet the authentication requirements. This does not preclude, however, that additional authentication and access controls may be deemed necessary by a system. These, however, would be imposed on users of a system in a uniform manner.

Regarding the validation and periodic reassessment of assurance levels, our certification and review procedures will include steps to validate that the technical solution employed achieve the required level of assurance and that assurance levels are periodically reassessed.

Appendix 3 – Principal Contributors to this Report

Peter J. Sheridan, Senior EDP Auditor and Project Lead

William L. Mitchell, Assistant Inspector General for Audits and Attestations